УДК 004.056.55
DOI: 10.25559/SITITO.14.201803.573-577

# THEORETICALLY UNBREAKABLE CIPHERS AS THEY SHOULD BE UNDERSTOOD

Alexander V. Babash[1], Valery A. Sizov[1], Elena K. Baranova[2], Andrey A. Mikrukov[1]
[1] Plekhanov Russian University of Economics, Moscow, Russia
[2] National Research University – Higher School of Economics, Moscow, Russia

# ТЕОРЕТИЧЕСКИ СТОЙКИЕ ШИФРЫ И КАК ИХ ПОНИМАТЬ

А.В. Бабаш[1], В.А. Сизов[1], Е.К. Баранова[2], А.А. Микрюков[1]
[1] Российский экономический университет имени Г.В. Плеханова, г. Москва, Россия
[2] Национальный исследовательский университет «Высшая школа экономики», г. Москва, Россия



**Keywords**

Cipher; perfectly secret encryption scheme; unbounded computing power.

**Abstract**

Perfectly-secret ciphers according to the Claude Shannon's theory, which are considered as unbreakable, and more specifically random keystream ciphers, are discussed. An analysis of the sources mentioned in the reference list showed that all of them come to the point that the perfect ciphers according to Claude Shannon's theory are unbreakable.

The article introduces some concepts, such as: the probabilistic model of cipher; the perfect cipher, which is secure against a plaintext recovery ciphertext-only attack; the perfect cipher, which is secure against a key recovery ciphertext-only attack; effective plaintext or key recovery attack; ineffective plaintext or key recovery attack; decipherable model of cipher; undecipherable model cipher. The introduced concepts were used to clarify Shannon's mathematical model and to prove that a statement about unbreakability of the perfect ciphers according to the Claude Shannon's theory, including random keystream cipher, were wrong. The purpose of the article is to attract the attention of specialists to the problem of developing methods for decrypting Vizhener cipher and using them in solving the problem of determining the cipher key of a random gamming according to a ciphertext, as well as developing methods for estimating the complexity and reliability of deciphering the cipher class in question.

**Ключевые слова**

Шифр; совершенно секретные схемы шифрования; неограниченная вычислительная мощность.

**Аннотация**

В статье рассмотрены совершенные шифры на основе модели К. Шеннона, которые считаются не дешифруемыми шифрами, в частности, шифры случайного гаммирования. Анализ представленных в статье источников показал, что в них делается вывод о недешифруемости совершенных шифров по К. Шеннону. В статье введен ряд понятий, таких как: вероятностной модели шифра; шифра, совершенного по нападению на открытый текст при перехвате шифрованного текста; шифра, совершенного по нападению на ключ при перехвате шифрованного текста; эффективной атаки на открытый текст или ключ; неэффективной атаки на открытый текст или ключ; дешифруемой модели шифра; не дешифруемой модели шифра. С использованием введенных понятий уточнена математическая модель К. Шеннона и доказана ошибочность утверждения о недешифруемости совершенных шифров по К. Шеннону, в частности шифров случайного гаммирования. Целью статьи является привлечение внимания специалистов к проблеме развития методов дешифрования шифра Виженера и их использования в решении задачи определения ключа шифра случайного гаммирования по шифрованному тексту, а также разработки методов оценки трудоемкости и надежности дешифрования рассматриваемого класса шифров.

About the authors:

**Alexander V. Babash**, Dr. Phys.-Math. Sci., Full Professor, Professor of the Academic Department of Applied Information Technology and Information Security, Institute of Digital Economics, Plekhanov Russian University of Economics (36 Stremyanny Lane, Moscow 115093, Russia), ORCID: http://orcid.org/0000-0001-7578-6923, babash@yandex.ru

**Valery A. Sizov**, Dr of Technical Sci., Full Professor, Professor of the Academic Department of Applied Information Technology and Information Security, Institute of Digital Economics, Plekhanov Russian University of Economics (36 Stremyanny Lane, Moscow 115093, Russia), ORCID: http://orcid.org/0000-0002-4844-4714, sizovva@gmail.com

**Elena K. Baranova**, Senior Lecturer, Senior Lecturer at Department of Information Security, National Research University – Higher School of Economics (20 Myasnitskaya Str., Moscow 101000, Russia), ORCID: http://orcid.org/0000-0003-4650-2623, ekbaranova@hse.ru

**Andrey A. Mikrukov**, PhD in Technical Sci., Senior Lecturer, Senior Lecturer of the Academic Department of Applied Information Technology and Information Security, Institute of Digital Economics, Plekhanov Russian University of Economics (36 Stremyanny Lane, Moscow 115093, Russia), ORCID: https://orcid.org/0000-0002-8206-677X, Mikrukov.aa@rea.ru

## Preface

Searching of the links through the Yandex search system gives 22 mln. results on the request "perfect ciphers" and 43 mln. results on the request «schemes perfectly secret». Some of them related to the subject domain of information security were chosen for detailed analysis [1-29].

The book [1: 32] contains a definition (2.3) of the concept «perfectly secret cipher» as follows: "An encryption scheme over a message space M is perfectly secret if for every probability distribution over M, every message m ∈ M, and every ciphertext c ∈ C for which *P(c)* > 0:

p(m/c)=p(m).

(The requirement that *P(c)>0* is a technical one needed to prevent conditioning on a zero-probability event.)". Such ciphers were introduced by Claude Shannon [13], who called them perfectly secret.

## Goal of research

Our strategic aim is to draw attention of the information protection specialists to questions of cryptanalysis of the random keystream cipher (Vernam cipher) and particularly to the question of development of the Vigenère cipher decryption techniques and use them to determine a key of random keystream cipher from ciphertext.

## Substantiation of the perfectly secret ciphers unbreakability in the works cited

The next sources [1-11] present the results of considerations of various encryption schemes that are secure even when the adversary has unbounded computational power. Such schemes are called perfectly secret. Qualitative descriptions of the ciphers under consideration are submitted below.

«In this chapter, we look at the other extreme and study encryption schemes that are provably secure even against an adversary who has unbounded computational power. Such schemes are called perfectly secret» [1: 35].

«The hotline between the United States and the former Soviet Union was (is it still active?) rumored to be encrypted with a one-time pad. Many Soviet spy messages to agents were encrypted using one-time pads. These messages are still secure today and will remain that way forever. It doesn't matter how long the supercomputers work on the problem. Even after the aliens from Andromeda land with their massive spaceships and undreamed-of computing power, they will not be able to read the Soviet spy messages encrypted with one-time pads (unless they can also go back in time and get the one-time pads» [2: 26 ].

«The one-time pad is the only available for us encryption technique, the absolute security of which can be proved» [3: 104].

«Theoretically, perfectly secret cipher (in other words, absolutely unbreakable cipher) does exist, but the only such cipher is only one of the forms of the so called "one time pad", in which the plaintext is encrypted by combining it with the key, which is truly random, and available for us algorithm of the same length» [4: 22]. It seems like to prevent any misconception the authors of this work [4] dropped a hint of doubt: 'keys produced by some truly random number generator will be high-quality with a probability that does not differ from unity more than a negligible quantity'» [4: 23].

"Considering the issue of theoretical unbreakability of ciphers, somebody can pay no attention to the real cost of complexity aspects and time needed for breaking a cipher (that determines an approach to the practical security of the cryptosystem). Pride of place goes to the possibility in principle to get any information about plaintext or used key. For the first time ever this approach was investigated by Claude Shannon [13]. Examining that model of cipher with which we are already well acquainted, he considered a single ciphertext-only crypt attack. Let us follow his reasoning. As we already specified, the ultimate objective of any cryptanalyst is a message text or a cryptographic key. However, even some probabilistic information about the plaintext can be very useful. For example, even before looking at a ciphertext the cryptanalyst may have a priori information about message because of his assumption only that plaintext is written in English [5: 172].

Russian cryptanalysts consider these ciphers as theoretically unbreakable [9-11]. Authors of these sources insist that these ciphers are undecipherable by an adversary who has unbounded computational power. Following their approach, all other ciphers, i. e. imperfect ciphers, must be considered as decipherable ones. As a rule, they refer random keystream cipher as an example of perfectly secret cipher [1-13].

## Clarification of the concept of perfect cipher according to the Claude Shannon's theory

Let us introduce following terms and symbols:

*M* – a finite set, consisting of two or more elements, is called the plaintext space;

*K* – a finite set, consisting of two or more elements, is called the key space;

*C* – a finite set, consisting of two or more elements, is called the ciphertext space;

$(f_k)_{k\in K}$ – a set (family) of injective mappings;

$(f_k^{-1})_{k\in K}$ – inverse mappings for $(f_k)_{k\in K}$, if $(f_k(m)=c$, then $f_k^{-1}(c)=m$;

$f: M\times K\to C$ – surjective mapping, $f(m,k)=f_k(m)$;

$f_k(m)=c$ ($f(m,k)=c$) – encryption equation;

$(f_k^{-1}(c)=m$ – decryption equation;

$P(M=(p(m),m\in M)$ – discrete probability distribution over space *M*;

$P(K)=(p(k),k\in K)$ – discrete probability distribution over space *K*.

**Definition 1**. Let's consider an assembly of five introduced concepts

(M,K,C, $(f_k)_{k\in K}$, $(f_k^{-1})_{k\in K}$ P(M), P(K))

as a probabilistic model of the Claude Shannon's cipher (encryption scheme) or, for the sake of brevity, a cipher model.

For ease of explanation of ensuing results, we will suppose, that for any $m\in M$, $k\in K$, $c\in C$

*p(m)≠0, p(k)≠0, p(c)≠0.*

Probability distributions *P(M), P(K)* induce:

Probability distribution $P(C)=(p(c),c\in C)$ over space *C*;

Conditional probability distribution $P(C/m)=(p(c/m),c\in C)$ for every $m\in M$;

Conditional probability distribution $P(K/c)=p(k/c),k\in K$; $c\in C$.

Conditional probability distribution $P(C/k)=(p(c/k),c\in C)$ for every $k\in K$.

By way of the cipher model *(M,K,C,*$(f_k)_{k\in K}$,$(f_k^{-1})_{k\in K}$*, P(M), P(K))* example, we would refer to the random keystream cipher (Vernam cipher) model.

Suppose that $I=\{1,2,...,n-1,0\}$, $M=I^n$, $K=I^n$, $C=I^n$. For $f_k(m)=c$ an encryption equation is determined by the equality $c=y_1,y_2,...,y_L$, where $y_j=i_j+\gamma_j \pmod n$, $j\in\{1,2,...,L\}$, and decryption equation is determined by the equalities $y_j-\gamma_j+n=i_j \pmod n$, $j\in\{1,2,...,L\}$. A probability distribution *P(M)* is established over the plaintext space *M*, and an equiprobable distribution *P(M)* is established over the key space *K*.

The work [13] provides more clarity on the definition 2.3 of perfectly secret cipher, which was presented in [1] earlier, as follows.

**Definition 2**. A cipher model over a message space M and the key space *K* is the perfect cipher, which is secure against a plaintext recovery ciphertext-only attack if for established probability distributions over spaces *M* and *K* for every message m ∈ M, and every ciphertext c ∈ C it is true, that:

p(m/c)=p(m).

The need for such refinement of the definition is dictated by the fact that each cipher can have several models. For example, the simple substitution cipher is considered as an imperfect one, although according to the models used to encrypt a plaintext of unit length, when "units" may be single letters, this cipher must be considered as perfectly secret [13].

**Definition 3**. An attack (mode, method) to determine a plaintext *m* of cipher (i. e. solutions of the equations *f(m,k) = c* in the unknown *m* from the space *M*), that requires non-zero expenditures because of time needed and complexity aspects and leads to a meaningful effect with a non-zero probability is called an effective attack for recovery of plaintext *m* of cipher model from established ciphertext *c*. Otherwise the attack is called ineffective.

**Note 1**. A plaintext recovery attack by guessing is not called effective.

**Definition 4**. Cipher model is called undecipherable if the effective attacks to determine the plaintext of this cipher model from established ciphertext do not exist. Otherwise, a cipher model is called decipherable.

**Hypothesis 1**. An effective ciphertext-only attack for plaintext recovery really does exist for imperfectly secret cipher model, which does not perfectly secure against a plaintext recovery.

Effective attacks on ciphers are divided into two classes: keyless when attacks allow to determine a plaintext without determining a secret key, and attacks based on preliminary determining a secret key. In the latter case, at first a secret key must be determined, and then a plaintext is read through decryption of ciphertext by recovered key.

**Definition 5**. A cipher model over a message space M and the key space *K* is the perfect cipher, which is secure against a key recovery ciphertext-only attack if for established probability distributions over spaces *M* and *K* for every message m ∈ M, and every ciphertext c ∈ C it is true, that:

p(k/c) = p(k).

Similarly to the definitions 3 and 4, a concept of effective attack on the key space of the cipher model and a concept of undecipherable cipher model in relation to the key recovery ciphertext-only attack were introduced.

**Hypothesis 2**. An effective ciphertext-only attack for key recovery really does exist for imperfectly secret cipher model, which does not perfectly secure against a key recovery.

**Theorem 1**. An effective plaintext recovery attack does exist for the perfectly secret cipher model which is secure against a plaintext recovery ciphertext-only attack, and for the imperfectly secret cipher model, which is not perfectly secure against a key recovery ciphertext-only attack, if the conditions of hypothesis 2 are fulfilled.

**Proof**. According to the hypothesis 2, an effective key recovery attack does exist. Having a key it is possible to decrypt a ciphertext encrypted by this key and recover a plaintext.

**A random keystream cipher is a decipherable one**

Let's formulate and prove the following theorem.

**Theorem 1**. In the cases of non-equiprobable probability distribution over the plaintext space and equiprobable probability distribution over the key space, a model of random keystrean cipher is not perfectly secret against key recovery ciphertext-only attacking.

**Proof**. We know that an initial condition that the equality *p(k/c)=p(k)* for any values of the keys *k* in the ciphertext *c* is equivalent to condition that *p(c/k)=p(c)* for any values of *k* and *c*. The equality *p(c/k)=p(m)* is obvious for the plaintext *m*, which was encrypted by the key *k* into ciphertext *c*. The statement of the theorem follows straightly from the condition of non-equiprobable probability distribution over the plaintext space. Consequently, a random keystream cipher must be considered as decipherable one.

**Note 2**. A key space is a subset of the key space of the random keystream ciphers. Let's call them weak keys. Known attacks on the Vigenère cipher are the attacks on the random keystream cipher with a key of smaller length. For example, an attack "favorable event method", i.e. searching applied weak key through the use of attack «the Father or Dean of American Cryptology William Frederick Friedman», can be applied [13]. Description of refining of the attack is presented in [13]. Such an attack provides the opportunity to find cipher texts encrypted by locally periodic stream [13]. Along with attack «William Frederick Friedman» another attack «Friedrich Wilhelm Kasiski» (see «Die Geheimschriften und die Dechiffrirkunst») can be applied.

Calculation of the complexity parameters for decryption of the random keystream cipher goes beyond the scope of the present study. Therefore, we believe that some special study should focus on that question.

**Theorem 2** (it had been formulated according to the personal communication with Aliev F. K.). A random keystream cipher $I=\{1,...,|I|-1,0\}$ is undecipherable one in the cases of equiprobable probability distribution over the plaintext space $M=I^N$ and over key space $K=I^N$.

The proof is obvious.

**The results**. On the basis of the reasoning submitted, we proved that the random keystream cipher is a decipherable one. Theoretically, it is necessary to develop appropriate methods for labor consumption estimation and reliability of deciphering the random keystream cipher.

## Conclusion

Formalization of concepts of breakability and unbreakability presented in this article, as well as statements submitted on their basis, allow us to conclude that an opinion about unbreakability of all perfectly secret ciphers is wrong. Further developing and improving research in the field of decryption techniques can provide a good solution of their use to determine a key of random keystream cipher from ciphertext.

## References

[1] Katz J. Lindell Y. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008. 553 p.
[2] Schneier B. Applied Cryptography. Second Edition: Protocols, Algorthms, and Source Code in C. John Wiley & Sons, 1996. 666 p.
[3] Schneier B. *Secrets & Lies*. Digital Security in a Networked World. John Wiley & Sons, 2000. 432 p.
[4] Zapechnikov S.V., Kazarin O.V., Tarasov A.A. Cryptographic Methods of Information Protection. M.: Urait, 2018. 309 p. (In Russian)
[5] Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V. Basics of Cryptography. M.: Gelios ARV, 2002. 480 p. (In Russian)
[6] Schneier B. Practical Cryptography. John Wiley & Sons, 2003. 432 p.
[7] Henk C.A. van Tilborg, Jajodia S. Encyclopedia of Cryptography and Security. Springer US, 2011. 1416 p.
[8] Godlewsky P., Minimal K. Cryptosystems for Unconditional Secrecy. *Journal of Cryptology*. 1990; 3(1):1-25. DOI: 10.1007/BF00203966
[9] Zubov A.Yu. Perfect Ciphers. M.: Gelios ARV, 2003. 160 p. (In Russian)
[10] Vasil'eva I.N. Cryptographic Methods of Information Protection. M.: Urait, 2016. 349 p. (In Russian)
[11] Zhdanov O.N., Zolotarev V.V. Methods and Tools of Cryptographic Protection of Information. Siberian State Aerospace Univ., Krasnoyarsk, 2007. 217 p. (In Russian)
[12] Babash A.V. Generalized Cipher Model. Intellectual Systems in the Information Confrontation. *Proceedings of the Russian Scientific Conference with International Participation.* December 8 -11, 2015. Moscow, Plekhanov Russian University of Economics, 2015. Pp. 9-14. (In Russian)
[13] Babash A.V., Shankin G.P. Cryptography. M.: Solon-Press, 2007. 512 p. (In Russian)
[14] Johansson T., Jonsson F. On the complexity of some cryptographic problems based on the general decoding problem. *IEEE Transactions on Information Theory*. 2002; 48(10):2669-2678. DOI: 10.1109/TIT.2002.802608
[15] LiangcY., Poor H.V., Shamai S. Information Theoretic Security. *Foundations and Trends R in Communications and Information Theory*. 2009; 5(4–5):355–580. DOI: 10.1561/0100000036
[16] Maurer U., Wolf S. The intrinsic conditional mutual information and perfect secrecy. *Proceedings of IEEE International Symposium on Information Theory*. Ulm, Germany, 1997. P. 88. DOI: 10.1109/ISIT.1997.613003
[17] Moulin P., O'Sullivan J.A. Information-theoretic analysis of information hiding. *IEEE Transactions on Information Theory*. 2003; 49(3):563-593. DOI: 10.1109/TIT.2002.808134
[18] Stallings W. Cryptography and Network Security: Principles and Practice. 5th ed. Pearson, Prentice Hall, Boston, 2011. 744 p.
[19] Stinson D.R. Cryptography: Theory and Practice, 3rd ed. (Discrete Mathematics and Its Applications). Chapman and Hall/CRC, 2006. 616 p.
[20] Trappe W., Washington L.C. Introduction to Cryptography with Coding Theory, 2nd ed. Prentice-Hall, Upper Saddle River, 2006. 577 p.
[21] Beimel A. Secret-Sharing Schemes: A Survey. Y.M. Chee et al. (Eds.) *Coding and Cryptology*. IWCC 2011. LNCS. Vol. 6639. Springer, Berlin, Heidelberg, 2011. Pp. 11–46. DOI: 10.1007/978-3-642-20901-7_2
[22] Carlet C., Ding C., Yuan J. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Transactions on Information Theory*. 2005; 51(6):2089-2102. DOI: 10.1109/TIT.2005.847722
[23] Cramer R., Damgard I., Maurer U. General Secure Multi-Party Computation from Any Linear Secret-Sharing Scheme. B. Preneel (Ed.) *Advances in Cryptology — EUROCRYPT 2000*. EUROCRYPT 2000. Lecture Notes in Computer Science. Vol. 1807. Springer, Berlin, Heidelberg, 2000. Pp. 316–334. DOI: 10.1007/3-540-45539-6_22
[24] Cohen G.D., Mesnager S., Patey A. On Minimal and Quasi-minimal Linear Codes. M. Stam (Ed.) *Cryptography and Coding*. IMACC 2013. Lecture Notes in Computer Science. Vol. 8308. Springer, Berlin, Heidelberg, 2013. Pp. 85-98. DOI: 10.1007/978-3-642-45239-0_6
[25] Cohen G., Mesnager S. On Minimal and Almost-Minimal Linear Codes. *Proceedings of the 21st International Symposium on Mathematical Theory of Networks and Systems (MTNS 2014)*. Session "Coding theory". Groningen, Netherlands, 2014. Pp. 928-931. Available at: http://fwn06.housing.rug.nl/mtns2014-papers/fullPapers/0098.pdf (accessed 12.05.2018).
[26] Cohen G., Mesnager S. Variations on Minimal Linear Codes. R. Pinto, P. Rocha Malonek, P. Vettori (Eds.) *Coding Theory and Applications*. 4th International Castle Meeting, Palmela Castle, Portugal, September 15-18, 2014. CIM Series in Mathematical Sciences. Vol. 3. Springer International Publishing, 2015. Pp. 125-131. DOI: 10.1007/978-3-319-17296-5_12
[27] Ding K., Ding C. A Class of Two-Weight and Three-Weight Codes and Their Applications in Secret Sharing. *IEEE Transactions on Information Theory*. 2015; 61(11):5835-5842. DOI: 10.1109/TIT.2015.2473861
[28] Lee C.-Y., Wang Z.-H., Harn L., Chang C.-C. Secure Key Transfer Protocol Based on Secret Sharing for Group Communications. *IEICE Transactions on Information and Systems*. 2011; E94-D(11):2069–2076. DOI: 10.1587/transinf.E94.D.2069
[29] Stinson D.R. Cryptography: Theory and Practice. Third Edition. Boca Raton: Chapman & Hall/CRC, 2006. 593 p.

Submitted 12.05.2018; revised 10.08.2018;
published online 30.09.2018.

## Список использованных источников

[1] *Katz J. Lindell Y.* Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008. 553 p.
[2] *Schneier B.* Applied Cryptography. Second Edition: Protocols, Algorthms, and Source Code in C. John Wiley & Sons, 1996. 666 p.
[3] *Шнайер Б.* Секреты и ложь. Безопасность данных в цифровом мире [Пер. с англ. Н. Дубнова]. СПб.: Питер, 2003. 367 с.
[4] *Запечников С.В., Казарин О.В., Тарасов А.А.* Криптографические методы защиты информации. М.: Издательство Юрайт, 2018. 309 с.
[5] *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. 2-еизд., испр. и доп. М.: Гелиос АРВ, 2002. 480 с.

[6] *Schneier B.* Practical Cryptography. John Wiley & Sons, 2003. 432 p.
[7] *Henk C.A. van Tilborg, Jajodia S.* Encyclopedia of Cryptography and Security. Springer US, 2011. 1416 p.
[8] *Godlewsky P., Minimal K.* Cryptosystems for Unconditional Secrecy // Journal of Cryptology. 1990. Vol. 3, issue 1. Pp. 1-25. DOI: 10.1007/BF00203966
[9] *Зубов А.Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003. 160 с.
[10] *Васильева И.Н.* Криптографические методы защиты информации. М.: Издательство Юрайт, 2016. 349 с.
[11] *Жданов О.Н., Золотарев В.В.* Методы и средства криптографической защиты информации. СибГАУ: Красноярск, 2007. 217 с.
[12] *Бабаш А.В.* Обобщенная модель шифра / Под ред. Н.И. Баяндина // Интеллектуальные системы в информационном противоборстве: сборник научных трудов российской научной конференции с международным участием. 8-11 декабря 2015. М.: РЭУ им. Г. В. Плеханова, 2015. С. 9-14.
[13] *Бабаш А.В., Шанкин Г.П.* Криптография / Под ред. В.П. Шерстюка, Э.Л. Применко. М.: Солон-Пресс, 2007. 512 с.
[14] *Johansson T., Jonsson F.* On the complexity of some cryptographic problems based on the general decoding problem // IEEE Transactions on Information Theory. 2002. Vol. 48, issue 10. Pp. 2669-2678. DOI: 10.1109/TIT.2002.802608
[15] *LiangcY., Poor H.V., Shamai S.* Information Theoretic Security // Foundations and Trends R in Communications and Information Theory. 2009. Vol. 5, issue 4–5. Pp. 355–580. DOI: 10.1561/0100000036
[16] *Maurer U., Wolf S.* The intrinsic conditional mutual information and perfect secrecy // Proceedings of IEEE International Symposium on Information Theory. Ulm, Germany, 1997. P. 88. DOI: 10.1109/ISIT.1997.613003
[17] *Moulin P., O'Sullivan J.A.* Information-theoretic analysis of information hiding // IEEE Transactions on Information Theory. 2003. Vol. 49, issue 3. Pp. 563-593. DOI: 10.1109/TIT.2002.808134
[18] *Stallings W.* Cryptography and Network Security: Principles and Practice. 5th ed. Pearson, Prentice Hall, Boston, 2011. 744 p.
[19] *Stinson D.R.* Cryptography: Theory and Practice, 3rd ed. (Discrete Mathematics and Its Applications). Chapman and Hall/CRC, 2006. 616 p.
[20] *Trappe W., Washington L.C.* Introduction to Cryptography with Coding Theory, 2nd ed. Prentice-Hall, Upper Saddle River, 2006. 577 p.
[21] *Beimel A.* Secret-Sharing Schemes: A Survey / Y.M. Chee et al. (Eds.) // Coding and Cryptology. IWCC 2011. LNCS. Vol. 6639. Springer, Berlin, Heidelberg, 2011. Pp. 11–46. DOI: 10.1007/978-3-642-20901-7_2
[22] *Carlet C., Ding C., Yuan J.* Linear codes from perfect nonlinear mappings and their secret sharing schemes // IEEE Transactions on Information Theory. 2005. Vol. 51, issue 6. Pp. 2089-2102. DOI: 10.1109/TIT.2005.847722
[23] *Cramer R., Damgard I., Maurer U.* General Secure Multi-Party Computation from Any Linear Secret-Sharing Scheme / B. Preneel (Ed.) // Advances in Cryptology — EUROCRYPT 2000. EUROCRYPT 2000. Lecture Notes in Computer Science. Vol. 1807. Springer, Berlin, Heidelberg, 2000. Pp. 316–334. DOI: 10.1007/3-540-45539-6_22
[24] *Cohen G.D., Mesnager S., Patey A.* On Minimal and Quasi-minimal Linear Codes / M. Stam (Ed.) // Cryptography and Coding. IMACC 2013. Lecture Notes in Computer Science. Vol. 8308. Springer, Berlin, Heidelberg, 2013. Pp. 85-98. DOI: 10.1007/978-3-642-45239-0_6
[25] *Cohen G., Mesnager S.* On Minimal and Almost-Minimal Linear Codes. Proceedings of the 21st International Symposium on Mathematical Theory of Networks and Systems (MTNS 2014). Session "Coding theory". Groningen, Netherlands, 2014. Pp. 928-931. URL: http://fwn06.housing.rug.nl/mtns2014-papers/fullPapers/0098.pdf (дата обращения: 12.05.2018).
[26] *Cohen G., Mesnager S.* Variations on Minimal Linear Codes / R. Pinto, P. Rocha Malonek, P. Vettori (Eds.) // Coding Theory and Applications. 4th International Castle Meeting, Palmela Castle, Portugal, September 15-18, 2014. CIM Series in Mathematical Sciences. Vol. 3. Springer International Publishing, 2015. Pp. 125-131. DOI: 10.1007/978-3-319-17296-5_12
[27] *Ding K., Ding C.* A Class of Two-Weight and Three-Weight Codes and Their Applications in Secret Sharing // IEEE Transactions on Information Theory. 2015. Vol. 61, issue 11. Pp. 5835-5842. DOI: 10.1109/TIT.2015.2473861
[28] *Lee C.-Y., Wang Z.-H., Harn L., Chang C.-C.* Secure Key Transfer Protocol Based on Secret Sharing for Group Communications // IEICE Transactions on Information and Systems. 2011. Vol. E94-D, issue 11. Pp. 2069–2076. DOI: 10.1587/transinf.E94.D.2069
[29] *Stinson D.R.* Cryptography: Theory and Practice. Third Edition. Boca Raton: Chapman & Hall/CRC, 2006. 593 p.

Поступила 12.05.2018; принята в печать 10.08.2018;
опубликована онлайн 30.09.2018.

Об авторах:

**Бабаш Александр Владимирович**, доктор физико-математических наук, профессор, кафедра прикладной информатики и информационной безопасности, Институт цифровой экономики и информационных технологий, Российский экономический университет имени Г.В. Плеханова (115093, Россия, г. Москва, Стремянный пер., д. 36), ORCID: http://orcid.org/0000-0001-7578-6923, babash@yandex.ru

**Сизов Валерий Александрович**, доктор технических наук, профессор, кафедра прикладной информатики и информационной безопасности, Институт цифровой экономики и информационных технологий, Российский экономический университет имени Г.В. Плеханова (115093, Россия, г. Москва, Стремянный пер., д. 36), ORCID: http://orcid.org/0000-0002-4844-4714, sizovva@gmail.com

**Баранова Елена Константиновна**, доцент, кафедра информационной безопасности, Национальный исследовательский университет «Высшая школа экономики» (101000, Россия, г. Москва, ул. Мясницкая, д. 20), ORCID: http://orcid.org/0000-0003-4650-2623, ekbaranova@hse.ru

**Микрюков Андрей Александрович**, кандидат технических наук, доцент, кафедра прикладной информатики и информационной безопасности, Институт цифровой экономики и информационных технологий, Российский экономический университет имени Г.В. Плеханова (115093, Россия, г. Москва, Стремянный пер., д. 36), ORCID: http://orcid.org/0000-0002-8206-677X, Mikrukov.aa@rea.ru